ARE YOU READY?
NEWSLETTER
Courtesy of the U. S. Fire Administration

Informing Communities of Organizational Y2K Planning

What role are fire and emergency service organizations taking in your community plan? Inform the public of your Y2K and disaster preparedness in a variety of ways.

- Facts and instructions can be included in utilities and banking statements, newspapers, radio, State and local educational TV networks, and tourism centers.
- Publicize to citizens not to make any ***non-emergency phone calls*** near midnight on December 31st to avoid line overload that could create confusion that something is wrong with the phones, when in reality, ***nothing is***.
- Provide printed information about Y2K and disaster preparedness to schools to send home with students.
- Make several model "72 hour kits" of basic emergency, nutritional and hygiene supplies that can be displayed at civic and business locations.

Share your department's Y2K activities on *the NEW USFA* comment form at www.usfa.fema.gov/y2k/.

USFA MATERIALS

The Millennium Fire-Safe Fact Sheet

Examines potential dangers such as stockpiling flammable fuel and faulty use of generators and alternative heating sources. The Fact Sheet is available in English and Spanish. Bulk copies may be ordered and customized by adding your own department label.

Y2K Contingency Planning Brochure

Emphasizes the importance of contingency planning to minimize the threat to the public and infrastructure. It addresses responder personal preparedness and lists a number of other planning resources.

Both are available free at (301) 447-1328 or through the USFA Web site at www.usfa.fema.gov/y2k/.

Y2K Public Preparedness Outreach Grants

In October, grants were made available to each State and territory to support Y2K public awareness, outreach and preparedness activities. Specifically, the grants were provided to support:

- Y2K awareness and preparedness seminars, conferences, and meetings.
- Completion of Y2K contingency planning by communities.
- Participation of States in local Y2K outreach activities, conferences, and meetings.
- Delivery of FEMA Y2K training materials to emergency managers and other appropriate individuals.
- Y2K tabletop drills and other exercises.
- Printing of Y2K materials to support outreach campaigns activities.
- Preparing State and local emergency management agencies in the use of the unique Y2K situation/incident reporting system and data base provided by the White House's Y2K Information Coordination Center through FEMA.

The grants were provided to the Emergency Management Director of each State. For information on how the grants are being used in your State and how your local agencies may be able to benefit from these activities, contact your State Emergency Management Director. For assistance locating a State Emergency Management Director, visit this web site:

http://www.nemaweb.org/State_Contacts/index.cfm

www.usfa.fema.gov/y2k/
(301) 447-1328
USFA Y2K INFORMATION OFFICE
16825 South Seton Avenue.
Emmitsburg, Maryland 21727

Presidential Decision Directive No.63 Critical Infrastructure

Critical infrastructures are the physical and cyber assets, processes and organizations that supply and distribute the vital goods and services upon which the nation's health, wealth and security rely. Power plants and power distribution grids, banks and financial institutions, water supplies, and information and communication systems are examples of these critical infrastructures. Much work in identifying critical cyber systems was accomplished by industry and government during preparations for Y2K conversion.

Presidential Decision Directive No. 63 (PDD-63), The Clinton Administration's Policy on Critical Infrastructure Protection, dated May 1998, was created to heighten awareness and to protect against the possibility of physical and cyber attacks on the nation's critical infrastructures. PDD-63 directed Federal departments and agencies to develop and implement plans to protect government operated information systems and assets and to work with industry to ensure the protection of key physical and cyber assets in critical infrastructure sectors. PDD-63 establishes a national goal for achieving the ability to protect the nation's critical infrastructure from intentional attacks (both physical and cyber) by the year 2003.

As members of the fire service, your organizations are associated with two of the twelve infrastructure areas identified by PDD-63 as critical to the functioning of the country- **Emergency Fire Service, and Public Health Services (including emergency medicine)**. The lead Federal agency for Emergency Fire Service is the Federal Emergency Management Agency (FEMA). The Department of Health and Human Services is the lead agency for Public Health Services (including emergency medicine). Each lead Federal agency is responsible for working with their critical infrastructure sector and appointing a liaison to the private organizations within their critical sectors.

For more information about security issues and infrastructure resources, visit these Internet sites:

www.ciao.gov.ncr.gov/

www.pccip.ncr.gov/

Emergency Services as Critical Infrastructures

Every community depends on emergency service and public safety providers for environmental and life safety. Most emergency service organizations now rely on high tech computer databases, as well as dispatch and telecommunications networks to enhance the delivery of those critical services.

Fire and emergency service organizations must protect system vulnerabilities within your operations, processes and physical environment. PDD-63 envisions identification of vulnerabilities that are exploitable by foreign or domestic computer hackers, disgruntled employees, or saboteurs.

The public safety answering point (PSAP/911) sector addresses exposures of telecommunication systems to accidental or intentional failures in lines, cable trunks and computer networks. Interruptions result in failures in the dispatch network.

Y2K preparations resulted in the replacement of some 911 systems and computer networks, resulting in compliance with the date-change. However, the vulnerability of the 911 network to foes worse than backhoes is just coming to light. There are significant exposures within the computer and communications systems themselves to intentional hacking and cyber interruptions.

Safe and successful fire and emergency responses depend on receiving a dispatch to the correct location in a timely manner. Databases provide firefighters with information on the scene location, structure design and potentially hazardous contents of businesses, transporting vehicles and industry. Personnel records or arson investigation documents, within your station or EOC should be considered important parts of your information infrastructure as well. Database loss or corruption or interruptions occurring in computer/ telecommunication networks compromise the life safety of both the potential victims at the scene and the emergency responders. The public's confidence in the emergency response network then diminishes.

Stay alert to areas of cyber or physical exposure in your emergency service infrastructure.

Y2K and HAZMAT Consequences

There may be more cause for Y2K concern in the chemical manufacturing sector than anticipated earlier in 1999. In October, the Senate Special Committee on the Year 2000 Technology Problem released a report that did not indicate adequate preparation or contingency planning by small and medium-sized chemical businesses. The report is available through the Internet sites, Year2000@y2k.senate.gov http://y2k.senate.gov/documents/sme_chemrpt.pdf.

Committee Vice-Chair, Senator Dodd, acknowledged that time is running out. "Developing viable Y2K contingency plans in conjunction with State and local officials must be a top priority in the chemical industry. "

A U.S. Chemical Safety Board member urged that plant managers, workers and emergency responders must redouble their efforts to coordinate contingency planning and implementation.

Fire and emergency service providers prepare for and encounter hazardous chemicals during responses 365 days a year.

Some conditions that make Y2K unique are:

- Potentially multiple toxic release events
- Reduced ability to provide mutual aide
- Contributing weather related hazards
- Potential for interruption of key utilities and telecommunications
- Threat of *intentional* disruptions in society and critical infrastructures.
- Potential loss of database sources for building contents/industrial components and hazardous materials indexing.
- Potential for loss of ALI or ANI if 911 operates on manual mode.

The emergency service sector can create awareness in their communities of hazards that are addressed through remediation and mutual contingency planning. A number of large chemical manufacturers plan to suspend, or limit, chemical processing operations over New Year's Eve as a precautionary move.

Find out what the chemical companies in your rural or urban communities have done to prepare for Y2K, if they are not part of your community-wide response and contingency planning effort.

To learn more about Y2K and hazardous chemical consequences,

visit these Internet sites:

http://www.fema.gov/fema/news.htm

http://www.chemsafety.gov/y2k/

http://www.epa.gov/ceppo/y2k.htm

http://www.senate.gov/~y2k/

http://www.osha-slc.gov/html/oshay2kpage.html

http://www.iaffhazmat.org/html/y2k_preparedness.html

Emergency Support in the Millenium Change Over

As part of the Federal Government's heightened readiness for Y2K, the interagency Emergency Support Team (EST) will be activated at FEMA Headquarters beginning December 28, along with the 10 FEMA Regional Operations Centers (ROCs), to monitor the unfolding situation. Numerous Federal agency Emergency Operations Centers (EOCs) and all State EOCs will be activated. Many emergency teams will be on alert. FEMA will deploy a Liaison to each State EOC, upon request, to assist the State in reporting on Y2K impacts, assessing resource needs and possible shortfalls, and developing a request for a Presidential emergency declaration if required. Federal agencies are hoping for the best but taking precautionary, prudent steps to prepare for any contingencies.

At all levels, government agencies are:

- Reaching out to the private sector,
- Updating emergency operations plans and procedures,
- Strengthening working relationships both horizontally and vertically.

USFA Y2K WEBSITE COMMENTS and LESSONS LEARNED

The updated USFA Y2K comment form at www.usfa.fema.gov.y2k provides a format for fire organizations to share tips on how disaster and Y2K preparedness messages are delivered to communities. Many respondents offer to be a resource point of contact for other departments or organizations.

Use the website e-mail response to share your successes and suggestions. Thanks to all those organizations and individuals who are providing information or contingency planning help to those requesting a point of contact.

The comment form asks what your fire or emergency service organization has done/is doing to promote public preparedness and safety for Y2K. How has your department informed your community about the readiness of emergency services for Y2K?

For operational preparations, consider these suggestions. Check wireless phones in the operational setting that you plan to use them in. For example, will they get good reception in the basement bunker, control center or the vehicles you plan to "Y2K Watch" and report from? In addition to generator power, are there sufficient dedicated emergency electrical outlets in your EOC and multiple connections for lap top computers?

Direct comments or questions to:

http://www.usfa.fema.gov/y2k/y2kform.htm

Contact the USFA Y2K Information Office at:

(301) 447-1328

Are school buses available in your community to provide transportation to large groups of people? Does your community contingency plan provide a way to shuttle individuals from celebrations or to comfort areas with utilities and services in event of service interruption due to Y2K or cold weather? Consider insurance issues. Would additional fire department driver-operators be permitted to use the ground transportation?

Create a public information office for your area and staff it during the rollover, regardless of the size of your community. Public safety announcements and press releases can be coordinated from a central area. In advance, invite community government, public safety and emergency service providers to discuss the release of information. Consider the environmental and security needs of the staff and providers in service over the New Year transition.

Find out what else is going on to build prepared communities at these Internet Sites:

- **FCC Y2K Emergency Service Links**
  http://www.fcc.gov/year2000/emerser.html#911
- **Montgomery County, Maryland**
  http://www.co.mo.md.us/pio/y2k/
- **The Red Cross**
  http://www.redcross.org/Y2K.html
- **USFA**
  http://www.usfa.fema.gov/y2k/y2kbest.htm
- **USFA**
  http://www.usfa.fema.gov/pdf/y2kcp.pdf

"Y2K and You" New Publication

The new publication "Y2K and You", is being distributed by FEMA to the emergency management community. The President's Council on Y2K is responsible for distribution to the general public as well as to governors, State Y2K Coordinators, Congress, national news media associations, and other groups. Emergency service providers and the public may order the publication at **1-888-USA-4Y2K**. It is also available for viewing and downloading at **www.fema.gov/y2k**.